SAV FSA

Schweizerischer Anwaltsverband
Fédération Suisse des Avocats
Federazione Svizzera degli Avvocati
Swiss Bar Association

Indications et recommandations de la FSA pour la sous-traitance informatique et l'utilisation de services *cloud*

I. Remarques liminaires

Aujourd'hui déjà, une étude d'avocats ne saurait s'organiser efficacement sans infrastructure informatique appropriée. Dans les prochaines années, cette nécessité se renforcera avec la numérisation croissante du flux de travaux des avocats. Afin de garantir un fonctionnement sûr et rentable du matériel et des logiciels utilisés, de plus en plus d'avocats feront appel à des services professionnels externes. Cette sous-traitance informatique, où le fournisseur agit en qualité d'auxiliaire de l'avocat, consiste à gérer et stocker les données de celui-ci, de même qu'à en organiser l'accès. La plupart du temps, ces services sont proposés via Internet, sous la forme d'un *cloud* (ci-après : services *cloud*).

1 La doctrine dominante retient que les fournisseurs de services *cloud* sont des auxiliaires de l'avocat[1]. De son côté, la Fédération Suisse des Avocats (FSA) constate que la sous-traitance informatique et les services *cloud* sont déjà la norme dans l'ensemble du secteur industriel et des prestataires de services. Pour les études d'avocats, ces services *cloud* apportent eux aussi des ***avantages*** incontestables, dont voici la synthèse :

- Par une informatique gérée professionnellement, renforcement de la sécurité des composants matériels et des données exploitées ;

[1] Christian Schwarzenegger / Florent Thouvenin / Burkhard Stiller / Damian) George, Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte, Revue de l'avocat 1/2019, p. 28 s.

- Économie dans l'engagement d'informaticiens et l'achat de matériel informatique ;
- Développement continu des fonctionnalités et fiabilité de l'infrastructure informatique ;
- Accès simplifié à l'infrastructure informatique.

2 La sous-traitance informatique et les services *cloud* s'accompagnent inévitablement d'une perte de contrôle (présumée) des données et des systèmes, entraînant de nouveaux ***risques potentiels***, dont les principaux sont les suivants :

- Violation des obligations professionnelles, en particulier celle du secret professionnel de l'avocat ;
- Non-conformité avec le droit de la protection des données ;
- Impondérables inhérents à l'externalisation contractuelle de services (contrôle des données et de leur stockage, appel à d'autres sous-traitants par le fournisseur cocontractant, contrôle de la sécurité des données, garantie de l'accès aux données).

3 Pour l'étude d'avocats, la sous-traitance informatique et l'utilisation de services *cloud* comportent ainsi leur lot d'incertitudes : à quelles conditions peut-on faire appel à ces services, quelles en sont les limites et comment minimiser les risques précités ? Autrement dit, comment l'avocat reste-t-il en conformité avec les règles professionnelles (en particulier son secret professionnel) et d'autres dispositions (comme celles de la protection des données), alors que tout son *workflow* numérique a été externalisé ?

4 En publiant ces recommandations (sous la forme d'un guide de bonnes pratiques), la FSA souhaite définir, en adéquation des risques et autres aspects techniques, un certain nombre de comportements standard à adopter par l'avocat en cas de sous-traitance informatique et de services *cloud*. L'objectif est de contribuer à la sécurité juridique et de permettre aux avocats de continuer à fournir des services compétitifs, fiables et de haute qualité dans le contexte de la transition numérique, tout en respectant le cadre juridique.

5 Ces recommandations ont pour ambition de faciliter l'obtention et l'utilisation de services *cloud* et peuvent servir d'aide aux membres FSA. Elles présentent le cadre juridique et apportent un certain nombre d'explications pour dissiper les insécurités juridiques ou l'absence de jurisprudence face aux nouveaux défis posés par les services *cloud*. En marge de ces recommandations générales, il est important que les études d'avocats tiennent également compte de leurs propres risques et autres besoins particuliers.

II. Terminologie

- **Sous-traitance informatique** : externalisation de services par laquelle l'avocat confie à un fournisseur externe les activités et les structures informatiques de son étude. Les services *cloud* sont une forme de sous-traitance informatique.
- **Services *cloud* :** mise à disposition d'une infrastructure informatique (espace de stockage, performances informatiques, applications, etc.), sous la forme de services qui passent par des interfaces techniques et des protocoles Internet. Matériellement, l'infrastructure informatique ne réside donc plus sur des serveurs locaux, mais est fournie à distance par un fournisseur de services *cloud* qui opère via Internet. Les services *cloud* varient en fonction de leur déploiement (*cloud* privé, *cloud* public et type de cryptage).
- **Fournisseurs de services informatiques** : auxiliaires de l'avocat qui accomplissent de la sous-traitance informatique ou fournissent des services *cloud*.

III. Liste des recommandations

6 L'avocat doit s'assurer que l'infrastructure informatique de son étude et l'intervention de fournisseurs de services informatiques respectent bien les exigences réglementaires et légales applicables. Pour la profession d'avocat, il s'agit notamment de l'obligation de diligence[2], le secret professionnel[3], ainsi que d'autres obligations légales telles que celles de la protection des données. L'obligation de diligence constitue le fil conducteur pour le choix de l'infrastructure informatique, de même que pour la sélection, l'instruction et le contrôle du fournisseur de services informatiques.

A. Appel à un fournisseur de services informatiques

1. Diligence dans le choix du fournisseur

7 Le fournisseur de services informatiques occupera une position de première importance dans l'organisation de l'étude d'avocats. Avant de jeter son dévolu sur tel ou tel fournisseur, il incombera à l'avocat de le soumettre à plusieurs questions centrales, en particulier celle de savoir s'il sera en mesure d'accomplir les tâches confiées avec tout le sérieux et le professionnalisme qu'on peut attendre de lui. Les critères suivants sont déterminants :

- Sa capacité à exécuter le contrat ;
- Son expérience et sa réputation ;

2 Art. 12 let. a LLCA.

3 Art. 13 LLCA et 321 CP.

- Son siège et le lieu où il déploie ses activités ;
- Ses clients de référence sur le marché des avocats ou d'autres prestataires de services : le nombre d'études d'avocats ou d'autres détenteurs d'un secret professionnel qu'il exploite, leur taille, dans quels pays, … ;
- Sa situation financière (stabilité économique, solvabilité, fiabilité, propriétés et adéquation des fonds propres) ;
- Nombre d'informaticiens (pour le support et le développement) ;
- Degré de dépendance envers ses propres fournisseurs ;
- Transparence dans les informations fournies : le fournisseur informe-t-il l'avocat des réquisitions de données par des autorités nationales ou étrangères, des attaques sur ses serveurs ou dans ses centres de données, etc. ;
- Perspective de développement des solutions proposées ;
- Localisation précise de ses serveurs de stockage (en particulier s'ils sont à l'étranger) ;
- Sécurité matérielle et électronique des serveurs et du centre de données ;
- S'il s'agit d'une société, d'un groupe de sociétés ou de toute autre forme de présence *à* l'étranger (y compris un accès aux données *depuis* l'étranger) : examen de la législation civile et pénale applicable sur place, de même que toutes autres dispositions étrangères, en particulier les obligations de divulguer des données de clients (par exemple l'*US Cloud Act*).

8 La sélection du fournisseur de services informatiques doit se faire à la lumière de ses compétences professionnelles ainsi que de ses ressources financières et humaines. A cet effet, il convient de tenir compte des besoins informatiques de l'étude d'avocats. Le fournisseur doit garantir que l'infrastructure informatique envisagée ainsi que son fonctionnement répondent aux risques concrets, juridiques et économiques d'un stockage des données de l'avocat. Au regard de l'art. 211 LP, les précautions nécessaires doivent être prises en cas d'insolvabilité du fournisseur de services informatiques. En cas de faillite, les contrats doivent être conçus de manière à ce que l'accès aux données puisse être maintenu ou être transféré à un autre fournisseur, ou qu'une infrastructure dite de basculement soit mise en place.

9 Si le fournisseur cumule plusieurs fonctions informatiques à l'égard de l'avocat, il conviendra d'évaluer le risque d'une trop forte concentration auprès du même cocontractant.

2. Diligence dans l'élaboration du contrat

10 L'intervention du fournisseur de services informatiques doit reposer sur un contrat écrit. La FSA recommande l'utilisation de l'un des modèles qu'elle a préparés à l'attention de ses membres[4], à tout le moins comme fil conducteur durant la phase précontractuelle.

11 Voici les points dont l'avocat devra tenir compte dans sa relation contractuelle avec le fournisseur de services informatiques :

- *Si le fournisseur fait appel à ses propres sous-traitants* : cette sous-traitance doit être réglée contractuellement. Si l'avocat autorise des sous-traitants, ils doivent être énumérés nominativement, être soumis aux mêmes obligations et fournir les mêmes garanties que le fournisseur cocontractant ;
- *Localisation du traitement et du stockage des données* : le contrat précise le lieu où le fournisseur exécute ses services informatiques, où il accède aux données et où il est en droit de stocker les données ;
- *Clause de confidentialité* : le contrat doit prévoir une clause selon laquelle le fournisseur respectera le secret professionnel de l'avocat. Le fournisseur doit être informé qu'il intervient comme auxiliaire et qu'il est par conséquent soumis au secret professionnel (art. 321 CP et 13 LLCA). Il doit s'engager contractuellement à la plus stricte confidentialité ;
- *Protection des données* : le contrat doit garantir que les exigences applicables en matière de protection des données seront appliquées ;
- *Traitement et remise de données à des tiers* : le contrat pose le principe selon lequel l'avocat conserve en tout temps le contrôle des données et que celles-ci devront lui être restituées sur simple demande. Réglementation détaillée en cas de faillite du fournisseur, de résiliation du contrat ainsi que des obligations si des tiers exigent la production de données ;
- *Accès aux données* : le contrat précise (i) quand, (ii) à partir de quel endroit, (iii) à quelle fin et (iv) quels employés ou sous-traitants du fournisseur peuvent accéder aux données ;
- *Sécurité des données* : le contrat définit le niveau de protection et de sécurité des données durant leur transfert, traitement et stockage. Réglementation des obligations d'information du fournisseur de services informatiques si des failles de sécurité ont été constatées ou utilisées abusivement par des tiers ;
- *Service Level Agreement (SLA)* : le contrat spécifie en toute clarté les services à fournir, leur disponibilité et leur niveau de qualité. Les attributions de l'avocat et du fournisseur doivent être définies et limitées contractuellement, en particulier pour les parts de responsabilité découlant d'activités communes ;

4 https://www.sav-fsa.ch/fr/service/anwaeltin-anwalt-in-der-cloud.html

- *Sauvegardes et récupération des données / imprévus* : le contrat doit prévoir un mécanisme de sécurité garantissant un rétablissement à brève échéance de toutes les fonctions externalisées, en particulier un accès rapide aux données dans les cas d'urgence (sauvegarde des données, accès à la sauvegarde, connexions Internet alternatives) ;
- *Droits de donner des instructions et de procéder à des contrôles* : ces droits doivent être définis contractuellement entre les parties. L'avocat peut soumettre les services et l'infrastructure du fournisseur à un audit de sécurité des données et de respect des exigences contractuelles (maintien de la confidentialité, respect de la protection des données, etc.) ;
- *Durée contractuelle* : en cas de résiliation par le fournisseur, le délai doit être suffisamment large pour permettre à l'avocat de trouver des solutions de remplacement ;
- *Concours du fournisseur lors de la résiliation du contrat* : le contrat énumère les obligations du fournisseur pour accompagner l'avocat et faciliter la recherche d'un autre fournisseur de services (maintien de la conformité aux normes, soutien durant le transfert de données, etc.). Le rétablissement de la fonction externalisée doit être garanti.

3. Surveillance du fournisseur de services informatiques

12 Le respect des obligations centrales du fournisseur (respect du secret professionnel et utilisation des données uniquement à des fins d'exécution des contrats) doit faire l'objet d'une surveillance proportionnelle aux risques encourus[5].

13 Pour des études d'une taille raisonnable, il suffit généralement de faire appel à un expert indépendant pour vérifier le dispositif de sécurité du fournisseur de services *cloud*. Se référer à son *système de management de la qualité* est également possible, pour autant qu'il réponde aux normes ISO 9001, 27001 ou à une certification spécifique à la protection des données (par exemple GoodPriv@cy, OCPD:2014 ou ePrivacy)[6].

14 Quelle que soit la taille de l'étude, les avocats effectueront eux aussi des contrôles réguliers, dont :

- Est-il possible d'accéder aux sauvegardes et, cas échéant, de rétablir les données ?
- Le logiciel antivirus est-il à jour ?

15 En fonction de la taille et de l'activité de l'étude d'avocats, il peut être utile de disposer de son propre système de sécurité[7]. Dans ce cas, la fonction sous-traitée au fournisseur doit

[5] Christian Schwarzenegger / Florent Thouvenin / Burkhard Stiller / Damian George, op. cit., p. 32
[6] Christian Schwarzenegger / Florent Thouvenin / Burkhard Stiller / Damian George, op. cit., p. 31
[7] Christian Schwarzenegger / Florent Thouvenin / Burkhard Stiller / Damian George, op. cit., p. 29

être intégrée au système de contrôle ou de sécurité informatique de l'étude d'avocats. Ces systèmes doivent être conçus en fonction du profil de risque des données de l'étude d'avocats. Ce faisant, l'avocat doit systématiquement identifier, surveiller, quantifier et gérer les risques importants liés au fonctionnement de son infrastructure informatique et à sa sous-traitance. Dans le cas d'informations particulièrement sensibles, des mesures techniques et organisationnelles appropriées doivent être prises pour protéger ces données. Le respect des obligations de droit civil et professionnel nécessite de restreindre efficacement le groupe de personnes autorisées à accéder aux données du client. Enfin, des mesures suffisantes doivent être prises pour les sécuriser[8].

B. Information du client de l'avocat

16 Au regard du droit de la profession d'avocat et de la protection des données, l'intervention d'un fournisseur de services informatiques ne requiert pas obligatoirement le consentement préalable du client.

17 Pour contribuer à la sécurité juridique et par souci de transparence, il est toutefois conseillé d'informer les clients de la sous-traitance informatique et de l'utilisation de moyens de communication électroniques, que ce soit dans les procurations ou les documents contractuels du mandat. L'avocat obtient ainsi le *consentement* de son client. Cet accord ne requiert aucune forme particulière et peut être donné par actes concluants, par exemple lorsque le client commence lui-même à utiliser de tels services informatiques ou moyens de communication.

18 Dans la mesure où l'avocat utilise, dans l'exécution du mandat, certains services informatiques et moyens de communication électroniques (Skype, courrier électronique, Google Docs, Office 365, traitement de données à l'étranger, etc.), il convient d'en informer le client dans le contrat de mandat et de le rendre attentif, d'une manière générale, aux risques de sécurité des données. Si le client commence lui-même à utiliser de tels services, l'obligation de l'avocat devient caduque.

Dans ce contexte, nous suggérons d'inclure dans le contrat de mandat la clause suivante : « *Veuillez noter que, pour nos services, nous faisons appel à des fournisseurs de services informatiques externes, ainsi qu'à des fournisseurs de* cloud *avec des serveurs en Suisse [ou à l'étranger]. Nous utilisons également certains services informatiques et moyens de communication qui présentent des risques liés à la sécurité des données (courrier électronique,* Skype*,* Google Docs*,* DropBox*, etc.). Si vous souhaitez que nous prenions des mesures de sécurité spéciales pour vos données, il vous incombe de nous en informer* ».

Comité spécialisé FSA transmission numérique, juin 2019

[8] Christian Schwarzenegger / Florent Thouvenin / Burkhard Stiller / Damian George, op. cit., p. 29